



Subject	Date	Policy #
ITS Security Policy	November 2022	ITS-1.4
	<b>Application</b>	<b>Supersedes</b>
	ITS Security	ITS-1.3
	<b>Distribution</b>	
	All Departments	
<b>Recommended</b>	<b>Approved</b>	
 Preston D. Marx, VP Information Systems	 James I. Marshall, President & CEO	

## 1.0 Purpose

This policy defines the standards and procedures for the physical and logical security of ITS systems at Uintah Basin Healthcare. Particular emphasis is given to procedures around logging, monitoring and reporting threats or anomalies within the system. This policy addresses HIPAA statute 164.308(a)(1)(i) as well as PCI requirements listed in the scope.

## 2.0 Scope

The policy applies to all organization owned facilities or equipment. The same expectation of security is given to each area commensurate to the threat level and plausible exposure at each location.

The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, UBH's cardholder environment consists only of limited payment applications (typically registration workstations) connected to the internet but does not include storage of cardholder data on any computer system. Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements as defined in Self-Assessment Questionnaire (SAQ) A-EP, version 3.2 revision 1.1, released January 2017.

## 3.0 Policy

### Overview

Security is the responsibility of each employee at Uintah Basin Healthcare. We are entrusted to protect human lives, electronic health records and capital equipment within our organization. Appropriate procedures to prevent, detect, contain, and correct security violations are prescribed in this policy.

A member of UBH leadership will serve as the security official (Security Officer). The security officer is responsible for the development and implementation of the policies and procedures required by HIPAA, PCI and other governing security mandates. The security officer works collaboratively with the compliance officer and privacy officer to educate, investigate and execute security matters. Security Incidents should be reported immediately to the HIPAA Security Officer and a member of the ITS Department.

## **Prevention**

### **Training / Education**

Training related to technology security, PCI compliance and HIPAA security safeguards is conducted during new employee orientation and is repeated annually to all active employees. Key points of this policy are presented.

All Security and HIPAA-related actions and activities, Policies and Procedures documented are updated and stored in a single location. This is the Information Technology team drive. Approved policies are shared on the UBH intranet page for all employees to access and read.

### **Physical Access**

Physical Security is simple but often overlooked. Access to key network assets including: ITS offices, UBH Server Room, Network & Telecommunication interface points, perimeter network closets and service provider demarcation points will be limited to authorized support personnel. These locations are to remain locked and regularly audited for unauthorized access. The use of security badges or traditional keyed entry in these areas is required. Network cameras record access into the ITS offices and server room.

If access to a key network location is necessary for individuals not a part of the ITS team for example: (vendor technicians, housekeeping, other UBH employees) the visits will always be monitored by an ITS team member. There is a member accessible 24x7 through our on-call service. A log will be kept of all access to secure areas.

### **Mobile Device Security**

Personal mobile devices namely phones, PDA and tablets are generally not managed by the ITS team and are not given access to UBH private networks. When business justifies network access, the device must be registered by the ITS team.

### **PCI Workstations**

- Portions of PCI compliance such as: penetration testing, network security and auditing are met organization-wide and are in most cases covered in

other policies or procedures. Any additional requirements by PCI are addressed in the "ITS PCI Compliance Procedural Checklist." Any workstation that processes cardholder data must comply with the workstation prep section of the procedure.

## **Detection**

### **Audits**

In systems where HIPAA protected data is stored, regular audits are performed by the security committee taking a random sampling of patient charts and systems. In addition, any allegation of misuse is investigated and reported promptly. This audit includes assigning unique user IDs (including not sharing accounts, ensuring all user IDs are associated with a person), searching for inappropriate access and a high number of failed access attempts. We promptly address anomalies as needed

Uintah Basin Healthcare ITS conducts audits and risk assessments based upon NIST and HIPAA standards on a semi-annual basis. Results are reviewed by the senior management team, who may implement risk management plans as needed.

An annual HIPAA Security Risk Assessment is conducted focusing on ePHI specific security threats. These findings are shared with the board of trustees and the risk assessment or compliance audit related documentation is retained for at least 6 years from creation.

Policies and Procedures and documentation related to ITS Security are reviewed and updated at least every 3 years and as needed in response to changes in the security of ePHI.

Systems and Network administrators of Uintah Basin Healthcare will utilize several tools to ensure proper network security. They will analyze and troubleshoot monthly vulnerability threats found from Utah Telehealth Intrusion Prevention Systems and scans. Network devices will be kept on the latest stable IOS version. Ensure access, both physical and electronic, to network equipment is kept to a small authorized and knowledgeable group. The Technology Department will proactively look for threats and mitigate their risks.

## **Correction**

### **Violations**

Security violations that are discovered through the course of audits or regular monitoring follow the ITS Incident Response Policy: identification, severity classification, containment, eradication, recovery and root cause analysis

Please refer to the ITS Incident Response Procedure for more details.

Uintah Basin Healthcare takes threats to their internal network seriously. Anyone found doing activities that are a threat to the network, create a hole in security or are circumventing UBH security measures will be subject to corrective action up to and including termination. If necessary, Uintah Basin Healthcare also reserves the right to advise appropriate legal officials of any illegal violations.